

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
CELLULAR ACCOUNT FOR TELEPHONE
NUMBER (423) 208-8461 THAT IS
STORED AT PREMISES CONTROLLED BY
VERIZON WIRELESS

Case No. 1:20-mj-22

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, James C. Hixson, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Verizon Wireless a wireless provider headquartered at 180 Washington Valley Road, Bedminster, New Jersey, 07921. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Verizon Wireless to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a Task Force Officer for the United States Department of Justice Drug Enforcement Administration. I have been employed as a law enforcement officer for a total of approximately 24 years. I graduated from the Chattanooga Police Department Police Academy in 1995 and throughout my law enforcement service have been involved in many investigations of

various criminal activities including acting in an undercover capacity in order to purchase and seize illegal narcotics. I have served as a Task Force Officer with the Drug Enforcement Administration since November 2004. During this time, I have worked and participated in numerous criminal cases involving narcotics that have resulted in successful prosecutions in both federal and state court. A number of these successful prosecutions were made possible by state and federal Title III wiretap investigations. During my career, I have attended numerous police and narcotics investigation schools, including a week-long certification course on the utilization of wiretap investigations. I have received training from the U.S. Attorney General, the Drug Enforcement Administration, the Federal Bureau of Investigation, the Tennessee Bureau of Investigation, and various other federal, state, and local law enforcement agencies as well as private companies. These courses have involved the identification, investigation, cultivation, transportation, manufacture, detection and prosecution of illegal drugs and related activities. These courses have allowed me to keep abreast of drug enforcement efforts, case development, procedures and practices, general investigative measures, and other standardized methods of investigation involving drug offenses. I have also had opportunity to develop knowledge of the equipment, tactics and techniques used in the production, consumption, sale, and distribution of various narcotics. I have also testified in the United States District Courts of the Eastern District of Tennessee as an expert on the subject matter of Drug Trafficking Organizations and the day-to-day operations of narcotics traffickers.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 21, United States Code Section 846 and 841 have been committed by Ramon BELTRAN. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. Your affiant is aware of an ongoing criminal investigation of Ramon BELTRAN being conducted by DEA, TBI, Chattanooga Police Department (CPD), and the Hamilton County (Tennessee) Sheriff's Department (HCSO). This investigation has identified BELTRAN as cocaine distributor in Chattanooga, Tennessee.

7. In May 2019, your affiant began an investigation into George MCCLAIN for his involvement in distributing cocaine. Since that time, your affiant has utilized a confidential source (CS) to make a series of controlled purchases of cocaine from MCCLAIN. In addition, your affiant debriefed the CS and learned that MCCLAIN and other associates routinely utilize their cellular telephones to arrange cocaine transactions.

8. As a result of the controlled purchases, on June 18, 2019, Hamilton County Criminal Court Judge Don Poole issued a Court order requesting the telephone company activate pen register coverage of (310) 721-3742 (i.e., TT-1). On August 26, 2019, Hamilton County

Criminal Court Judge Don Poole issued a Court order requesting the telephone company to continue pen register coverage of (310) 721-3742 (i.e., TT-1). The Orders authorized the identification of numbers dialed from or pulsed to the Target Telephones for a period of 60 days.

9. On October 1, 2019, a federal application and order to intercept the wire and electronic communications of George MCCLAIN over TT-1 (310) 721-3742 was signed by the Honorable Judge Travis McDonough, United States District Judge, Eastern District of Tennessee. Interception of TT-1 began on October 1, 2019 and continued through December 2019. Blake HIGGINS was intercepted on the court authorized intercept utilizing telephone number (423)255-8821.

10. Through the investigation at the time of this affidavit, case agents have determined that HIGGINS utilized voice calls to MCCLAIN to arrange the purchase of cocaine. HIGGINS was intercepted on a number of occasions through voice calls that monitors determined to be "Pertinent" to the investigation. Your affiant has personally reviewed those voice calls and determined that HIGGINS was purchasing resale quantities of cocaine from MCCLAIN.

11. On February 11, 2020, TFO Hixson and TFO Dockery conducted surveillance of HIGGINS. TFO Hixson and TFO Dockery conducted surveillance on HIGGINS as he drove around various locations in Chattanooga, Tennessee. HIGGINS was ultimately followed to Hamilton Place Mall in Chattanooga, Tennessee. After surveilling HIGGINS inside Hamilton Place Mall it became clear to TFO Hixson that HIGGINS was waiting to meet someone. HIGGINS loitered around the mall for approximately 1 hour constantly text messaging with someone and talking on his cellular phone.

12. At approximately 4:35 PM, TFO Hixson observed HIGGINS walking out of the mall and into the parking lot near where he parked his vehicle. TFO Hixson observed HIGGINS

stop at Lexus SUV that had just parked on the row of parking spaces near where HIGGINS was parked. TFO Hixson then observed a Hispanic male exit the passenger side of the LEXUS SUV as a female and 2 juveniles got out of the vehicle and walked into the mall entrance. TFO Hixson observed the Hispanic male and HIGGINS get into HIGGINS vehicle and appeared to begin exchanging items between each other. TFO Hixson assisted by TFO Rodd Watters and TFO Dockery approached HIGGINS' vehicle. As HIGGINS observed law enforcement officers approaching HIGGINS quickly made a movement with his right hand down towards his lap and started his vehicle. TFO Hixson identified himself as a law enforcement officer and gave HIGGINS and the Hispanic male a command to show their hands. HIGGINS quickly reached toward the gear shifter and appeared to be trying to put the vehicle into reverse when TFO Hixson opened HIGGINS door and gave HIGGINS commands to exit the vehicle.

13. As TFO Hixson escorted HIGGINS from the vehicle, TFO Watters asked the Hispanic male to exit the passenger side of the vehicle. Once outside the vehicle, TFO Watters asked the Hispanic male if he had any weapons or anything that would stick him (TFO Watters) on his (Hispanic males) person. The Hispanic male responded he had cocaine in his right front pocket. TFO Watters asked the Hispanic male if he (TFO Watters) could retrieve the cocaine. The Hispanic male agreed and allowed TFO Watters to remove an envelope which contained small bags of what appeared to be cocaine. TFO Watters then retrieved the Hispanic male's wallet and identification. TFO Watters noted the wallet contained several \$100 bills. The identification revealed the Hispanic male was Ramon BELTRAN. TFO Watters issued BELTRAN his Miranda Warnings as witnessed by TFO Dockery. TFO Hixson spoke with BELTRAN about his residency and occupation. BELTRAN stated he sells cars and that stuff, referring to the cocaine. TFO Watters asked BELTRAN for consent to look through his cellular phone. BELTRAN granted consent and

provided TFO Watters with the code to unlock the phone, as witnessed by TFO Hixson. TFO Hixson noted a string of text messages between BELTRAN and "Blake Black", TFO Hixson confirmed that the contact "Blake Black" was the number (423)255-8821 the number utilized by HIGGINS. TFO Hixson also noted that the string of text messages contained messages where HIGGINS was requesting "2" and telling BELTRAN, "Need 2 break one down". TFO Hixson also noted several other series of text messages between BELTRAN and other individuals that confirmed BELTRAN was using the text messaging function of his cellular phone to conduct narcotic transactions with other individuals.

14. TFO Hixson confirmed BELTRAN's phone utilized telephone number (423) 208-8461.

15. TFO Hixson issued HIGGINS his Miranda Warnings as witnessed by TFO Dockery. HIGGINS stated he understood and agreed to cooperate with TFO Hixson. HIGGINS confirmed that he was at the mall to meet BELTRAN and purchase cocaine. HIGGINS also confirmed that BELTRAN was his current cocaine source of supply.

16. On February 12, 2020, a request to preserve text messages sent to and from (423) 208-8461 was sent to Verizon Wireless by DEA TFO James Hixson. On February 13, 2020, TFO Hixson received notification back from Verizon Wireless acknowledging the preservation of text messages as reflected in Verizon Wireless Case ID# 200039833.

17. In my training and experience, I have learned that Verizon Wireless is a company that provides cellular telephone access to the general public, and that stored electronic communications, including retrieved and unretrieved voicemail, text, and multimedia messages for Verizon Wireless subscribers may be located on the computers of Verizon Wireless. Further,

I am aware that computers located at Verizon Wireless contain information and other stored electronic communications belonging to unrelated third parties.

18. Wireless phone providers often provide their subscribers with voicemail services. In general, a provider will store voicemail messages on behalf of a particular subscriber until the subscriber deletes the voicemail. If the subscriber does not delete the message, the message may remain in the system of Verizon Wireless for weeks or months.

19. Among the services commonly offered by wireless phone providers is the capacity to send short text or multimedia messages (photos, audio, or video) from one subscriber's phone or wireless device to another phone or wireless device via one or more wireless providers. This service is often referred to as "Short Message Service" ("SMS") or "Multimedia Messaging Service" ("MMS"), and is often referred to generically as "text messaging." Based on my knowledge and experience, I believe that stored electronic communications, including SMS and MMS messages that have been sent or received by subscribers, may be stored by Verizon Wireless for short periods incident to and following their transmission. In addition, providers occasionally retain printouts from original storage of text messages for a particular subscriber's account.

20. Wireless phone providers typically retain certain transactional information about the use of each telephone, voicemail, and text-messaging account on their systems. This information can include log files and messaging logs showing all activity on the account, such as local and long distance telephone connection records, records of session times and durations, lists of all incoming and outgoing telephone numbers or e-mail addresses associated with particular telephone calls, voicemail messages, and text or multimedia messages. Providers may also have information about the dates, times, and methods of connecting associated with every communication in which a particular cellular device was involved.

21. Wireless providers may also retain text messaging logs that include specific information about text and multimedia messages sent or received from the account, such as the dates and times of the messages. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number (“ESN”), a Mobile Electronic Identity Number (“MEIN”), a Mobile Identification Number (“MIN”), a Subscriber Identity Module (“SIM”), an International Mobile Subscriber Identifier (“IMSI”), or an International Mobile Station Equipment Identity (“IMEI”). When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

22. Many wireless providers retain information about the location in which a particular communication was transmitted or received. This information can include data about which “cell towers” (i.e., antenna towers covering specific geographic areas) received a radio signal from the cellular device and thereby transmitted or received the communication in question.

23. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers’ full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service utilized, the ESN or other unique identifier for the cellular device associated with the account, the subscribers’ Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the

services available to the account subscribers. In addition, wireless providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates, times and sometimes, places, of payments and the means and source of payment (including any credit card or bank account number).

24. In some cases, wireless subscribers may communicate directly with a wireless provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Wireless providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

25. As explained below, information stored at the wireless provider, including that described above, may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the data pertaining to a particular cellular device that is retained by a wireless provider can indicate who has used or controlled the cellular device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, data collected at the time of account sign-up, information relating to account payments, and communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled a cellular device at a relevant time. Further, such stored electronic data can show how and when the cellular device and associated cellular service were accessed or used. Such “timeline” information allows investigators to understand the

chronological context of cellular device usage, account access, and events relating to the crime under investigation. This “timeline” information may tend to either inculpate or exculpate the cellular device owner. Additionally, information stored by the wireless provider may indicate the geographic location of the cellular device and user at a particular time (e.g., historic cell-site location information; location integrated into an image or video sent via text message to include both metadata and the physical location displayed in an image or video). Last, stored electronic data may provide relevant insight into the state of mind of the cellular device’s owner and/or user as it relates to the offense under investigation. For example, information relating to the cellular device in the possession of the wireless provider may indicate the owner’s motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

26. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Verizon Wireless to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

27. Based on the forgoing, I request that the Court issue the proposed search warrant.

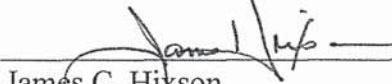
28. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

29. The government will execute this warrant by serving the warrant on Verizon Wireless. Because the warrant will be served on Verizon Wireless, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

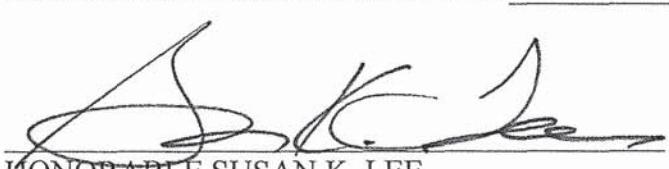
30. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed for 90 days. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,



James C. Hixson
Task Force Officer
Drug Enforcement Administration

Subscribed and sworn to before me on FEB. 20, 2020.


HONORABLE SUSAN K. LEE
UNITED STATES MAGISTRATE JUDGE

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
CELLULAR ACCOUNT FOR TELEPHONE
NUMBER (423) 208-8461 THAT IS
STORED AT PREMISES CONTROLLED BY
VERIZON WIRELESS

Case No. 1:20-mj- 22

Filed Under Seal

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with CELLULAR ACCOUNT FOR
TELEPHONE NUMBER (423) 208-8461 that is stored at premises owned, maintained,
controlled, or operated by Verizon Wireless, a wireless provider headquartered at 180
Washington Valley Road, Bedminster, New Jersey, 07921.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
CELLULAR ACCOUNT FOR
TELEPHONE NUMBER (423) 208-8461
THAT IS STORED AT PREMISES
CONTROLLED BY VERIZON WIRELESS

Case No. 1:20-mj- 22

Filed Under Seal

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Verizon Wireless

To the extent that the information described in Attachment A is within the possession, custody, or control of Verizon Wireless, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to Verizon Wireless or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Verizon Wireless is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. All voice mail, text, and multimedia messages **January 1, 2020 to February 13, 2020** stored and presently contained in, or on behalf of the account or identifier;
- b. All existing printouts from original storage of all of the text messages described above;
- c. All transactional information of all activity of the telephones and/or voicemail accounts described above, including log files, messaging logs, local and long distance telephone

connection records, records of session times and durations, dates and times of connecting, methods of connecting, telephone numbers associated with outgoing and incoming calls; cell towers used, and/or locations used from **January 1, 2020 to February 13, 2020**;

d. All text messaging logs, including date and time of messages, and identification numbers associated with the handsets sending and receiving the message **January 1, 2020 to February 13, 2020**;

e. All business records and subscriber information, in any form kept, pertaining to the individual accounts and/or identifiers described above, including subscribers' full names, addresses, shipping addresses, date account was opened, length of service, the types of service utilized, ESN (Electronic Serial Number) or other unique identifier for the wireless device associated with the account, Social Security number, date of birth, telephone numbers, and other identifiers associated with the account;

f. Detailed billing records, showing all billable calls including outgoing digits, from **January 1, 2020 to February 13, 2020**;

g. All payment information, including dates and times of payments and means and source of payment (including any credit or bank account number), from **January 1, 2020 to February 13, 2020**;

h. Incoming and outgoing telephone numbers, from **January 1, 2020 to February 13, 2020**;

i. All records indicating the services available to subscribers of individual accounts and/or identifiers described above;

j. All records pertaining to communications between Verizon Wireless and any person regarding the account or identifier, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 21, United States Code Sections 846 and 841 involving Ramon BELTRAN since January 1, 2020 including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Evidence relating to the sale and distribution of controlled substances.
- b. Evidence indicating how and when the cellular device and associated cellular service was used to determine the chronological context of cellular device use, account access, and events relating to the crime under investigation;
- c. Evidence indicating the geographic location of the cellular device at times relevant to the investigation;
- d. Evidence indicating the cellular device owner or user's state of mind as it relates to the crime under investigation;
- e. The identity of the person(s) who created the account associated with the cellular device and/or used the cellular device, including records that help reveal the whereabouts of such person(s)